Personally Identifiable Information

Personally identifiable information (PII) is any information that can be used to identify, contact, or locate an individual. Examples include:

- Name
- Social Security Number (SSN)
- Date of birth
- Home address
- Phone number
- E-mail address
- Account number
- Driver's license number
- Fingerprint
- Photograph

Any information associated with PII should be considered private and must be properly protected. Federal regulations and HHS policies dictate that PII must be protected when collected, accessed, used, stored, or transmitted. Whether you are working from your desk at the office or working off-site, it is your responsibility to ensure that the information entrusted to you in the course of your work is kept private and secure. This brochure provides some guidance on what steps you can take to keep private information private.

Vulnerable Locations for Information

Trash

- Dispose of un-needed or unwanted documents or diskettes containing sensitive data appropriately.
- Use caution when discarding information in your waste bin. Once trash leaves the office, we lose control over it, and it can become vulnerable.

Fax machines

- Double check fax numbers before dialing, and before transmitting, to ensure that you have it correct.
- Call the recipient BEFORE and AFTER the transmission for verification that it was received by the right person.

Vulnerable Locations for Information

Printers

- Verify printer location PRIOR to sending a document to the printer.
- Promptly pick up ALL copies of the documents.
- Dispose of sensitive documents by following your office's procedures.
- Use a special trash receptacle for sensitive papers or a paper shredder.

E-mail

- Make your default action "reply to sender" rather than "reply to all."
- Double check email addresses to make sure that you have selected the correct recipient.
- Double check your attachment to make sure that you have selected the correct document.
- If you are sending to multiple people or a distribution list, make sure that what you are sending is appropriate for every recipient.
- Confirm that sensitive data has been received properly.
- Do not send highly sensitive information via e-mail unless encrypted.
- Use a password lock for your machine when you are away from your desk.

External Storage Devices (Memory sticks, disks, CDs)

- Be sure to remove your storage device from public computers.
- Store your device in a safe place, to make sure that it is not lost or stolen.
- Do not store sensitive information on portable or external storage devices, including home computers, unless encrypted.

Public Places

- Do not discuss sensitive information in public places, such as restaurants, elevators, hallways, bathrooms, or outside of the Department.

Using Encryption

Encryption is the practice of converting information into a format that cannot be read without a key code. Decrypting information converts that information back into a readable format by using the key.

Learn how to use Encryption:

- Contact your Chief Information Security Officer (CISO) to learn about using encryption.

Encrypt any PII that is:

- Stored on your desk computer or laptop,
- Sent in an electronic mail, or
- Stored or transferred by a portable device to a remote site, including your home).

Storing and Accessing Information

- Store sensitive data in an encrypted format, whatever its source.
- Make sure that controls are in place to limit access to systems that contain sensitive data.
- Avoid storage of sensitive data on non-government systems, such as publicly accessible or personal computers.
- Make sure all data transfers, including downloads, occur only using secure or encrypted connections from trusted sources.
- Access sensitive data from secure computers only. Do not access sensitive data from public computers, such as those in hotels or business centers.
- Remove temporary files created when using the World Wide Web, such as those found in browser caches and temp files, especially when you are accessing information from a non-secure computer.

Please contact your Help Desk or SecureOne HHS at secureone.hhs@hhs.gov, for more information on how to protect your privacy at work.

Remote Access

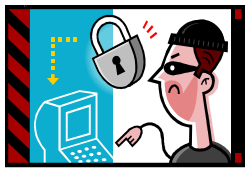
- Encrypt all sensitive data on mobile computers or devices which have appropriate safeguards to carry agency data
- Use two-factor authentication to access sensitive data remotely. This means two mechanisms are required in order to gain access, for example a password and a smart card.
- Use a "time-out" function requiring user re-authentication after 30 minutes of inactivity.

Loss of or unauthorized disclosure of private information costs time and money. In addition, a number of other

Reporting Security Incidents

issues can come about from the loss of private information. To mitigate these concerns, make sure you heed these tips when you suspect a security violation or other incident:

- Report ANY unauthorized disclosure involving sensitive information to your Chief Information Security Officer (CISO).
- IMMEDIATELY report all incidents, whether suspected or confirmed.
- DO NOT move, delete, or tamper with evidence.
- Note any unique circumstances.



For more Information:

For more information, contact your OPDIV Help Desk or Secure One HHS at secureone.hhs@hhs.gov or http://intranet.hhs.gov/infosec/.

Print OPDIV CISO name, office address, phone and email here, or appropriate contact information

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

U.S. Department of Health and Human Services

How to Protect Private Information